LAUR-06-5374

Invited Talk for the U.S.-Russia Joint TID Working Group
Moscow, Russia, September 13-14, 2006

Vulnerability Assessments of Tamper-Indicating Seals

Roger G. Johnston, Ph.D., CPP

Vulnerability Assessment Team
Los Alamos National Laboratory

505-667-7414 rogerj@lanl.gov
http://pearl1.lanl.gov/seals

LANL Vulnerability Assessment Team

Physical Security

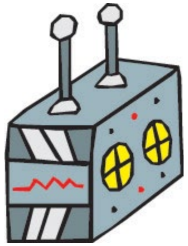
VAT

- consulting
- cargo security
- tamper detection
- training & curricula
- nuclear safeguards
- new tags, seals, & traps
- vulnerability assessments
- novel security approaches
- security psychological issues

The VAT has done detailed vulnerability assessments on hundreds of different security devices, systems, & programs.

> The greatest of faults, I should say,
> is to be conscious of none.
> -- Thomas Carlyle (1795-1881)

Security Maxims



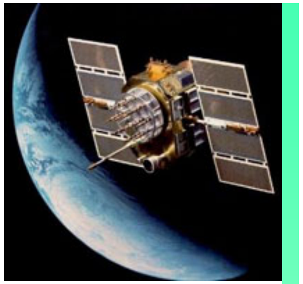
1. **Infinity Maxim**: There are an unlimited number of vulnerabilities, most of which will never be discovered (by the good guys or bad guys).

2. **Arrogance Maxim**: The ease of defeating a security device is inversely proportional to how confident the designer, manufacturer, or user is about it, and to how often they use words like “impossible” or “tamper-proof”.

3. **High-Tech Maxim**: The amount of careful thinking that has gone into a given security device is inversely proportional to the amount of high-technology it uses.

> Confidence is that feeling you sometimes have before you fully understand the situation. -- Anonymous

Security Maxims



4. **Low-Tech Maxim**: Low-tech attacks work (even against high-tech devices).

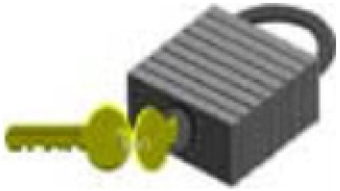
5. **Yes! Maxim**: There are effective, simple, & low-cost countermeasures to most vulnerabilities.

6. **Oh No! Maxim**: But users, manufacturers, and bureaucrats will be reluctant to implement them.

> If you think that technology can solve your security problems, then you don't understand the problems and you don't understand the technology. -- Bruce Schneier

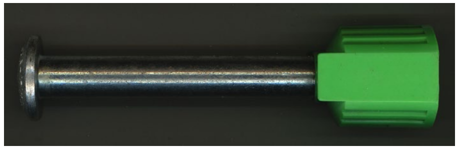
Terminology

lock: a device to delay, complicate, and/or discourage unauthorized entry.



(tamper-indicating) seal: a device meant to leave non-erasable, unambiguous evidence of unauthorized entry or tampering.

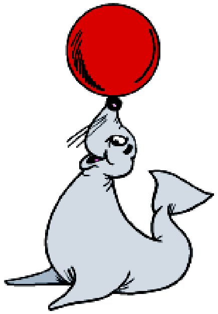
barrier seal: a device that is both a lock & a seal



> If I had only known, I would have been a locksmith.
> -- Albert Einstein (1879-1950)

Terminology

defeating a seal: opening a seal, then resealing (using the original seal or a counterfeit) without being detected.



attacking a seal: undertaking a sequence of actions designed to defeat it.

Defeating seals is mostly about fooling people, not beating hardware (unlike defeating locks, safes, or vaults)!

Terminology

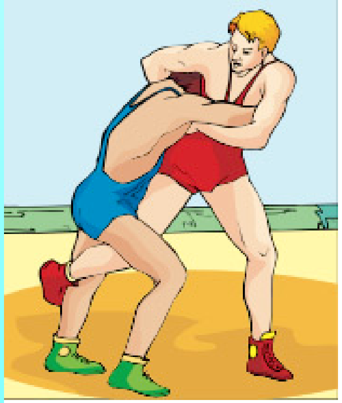
(seal) use protocol: the official as well as the unofficial & informal ways the seal is used. Includes procurement, shipping, storage, installation, inspection, removal, destruction, reporting, interpretation, & training.

<u>A seal is no better than its use protocol!</u>

seal countermeasures: ways to improve the seal by changing the design and/or the seal use protocol.

Terminology

vulnerability assessment (VA): discovering and demonstrating ways to defeat a seal or tamper-detection program. Should include suggesting countermeasures.



He that wrestles with us strengthens
our skill. Our antagonist is our helper.
-- Edmund Burke (1729-1797)

Vulnerability Assessments

The purpose is to improve tamper detection, not to:

- Pass a test
- Generate metrics
- Justify the status quo
- Check against some standard
- Claim there are no vulnerabilities
- Rationalize the research & development
- Certify a seal as “good” or “ready for use”
- Perform material, environmental, or quality tests
- Apply a mindless, bureaucratic stamp of approval
- Praise or accuse the developer, manufacturer, or user

> Nothing is easier than self-deceit. For what each man wishes, that he also believes to be true.
> -- Demosthenes (382-322 BC)

Seal Attacks

When choosing between two evils, I always pick the one I never tried before.
-- Mae West (1893-1980)

There are at least 105 different ways to attack seals, most in 1 of 10 categories:

Pick Attacks - Pick the seal open without damage or evidence.

Unsealing Attacks - Open the seal, then repair or hide any damage or evidence.

Backdoor Attacks - Put a defect in the seal prior to use.

Tampering with the Seal Data - Tamper with data (such as the seal serial number), or reports about the seal inspection.

Seal Reader Attacks - Tamper with, spoof, or counterfeit the electronic seal verifier (if any).

Seal Attacks

I told my psychiatrist that everyone hates me. He said I was being ridiculous--everyone hasn't met me yet. -- Rodney Dangerfield (1921-1997)

Electronic Attacks - For electronic seals, attack various components such as the sensors, microprocessor, signals, power, annunciator, encryption, or stored data.

Replicating - Make a duplicate seal at the factory using procurement, breaking & entering, bribery, coercion, or psychological means.

Counterfeiting - Make a duplicate seal outside of the factory.

Failure Mode Attacks - Challenge the seal security program directly or with misdirection, or wait until an error is made and then exploit it.

Sabotage the Sealing Process - Corrupt the sealing process, such as applying the wrong seal, failing to seal properly, or not closing the door or lid.

Fake Counterfeits

Often overlooked: an adversary often needs only to mimic the superficial appearance and perhaps simulate the apparent performance of a seal or reader. This is much easier than true counterfeiting.

> Sincerity is everything. If you can fake that, you've got it made.
>
> -- George Burns (1896-1996)

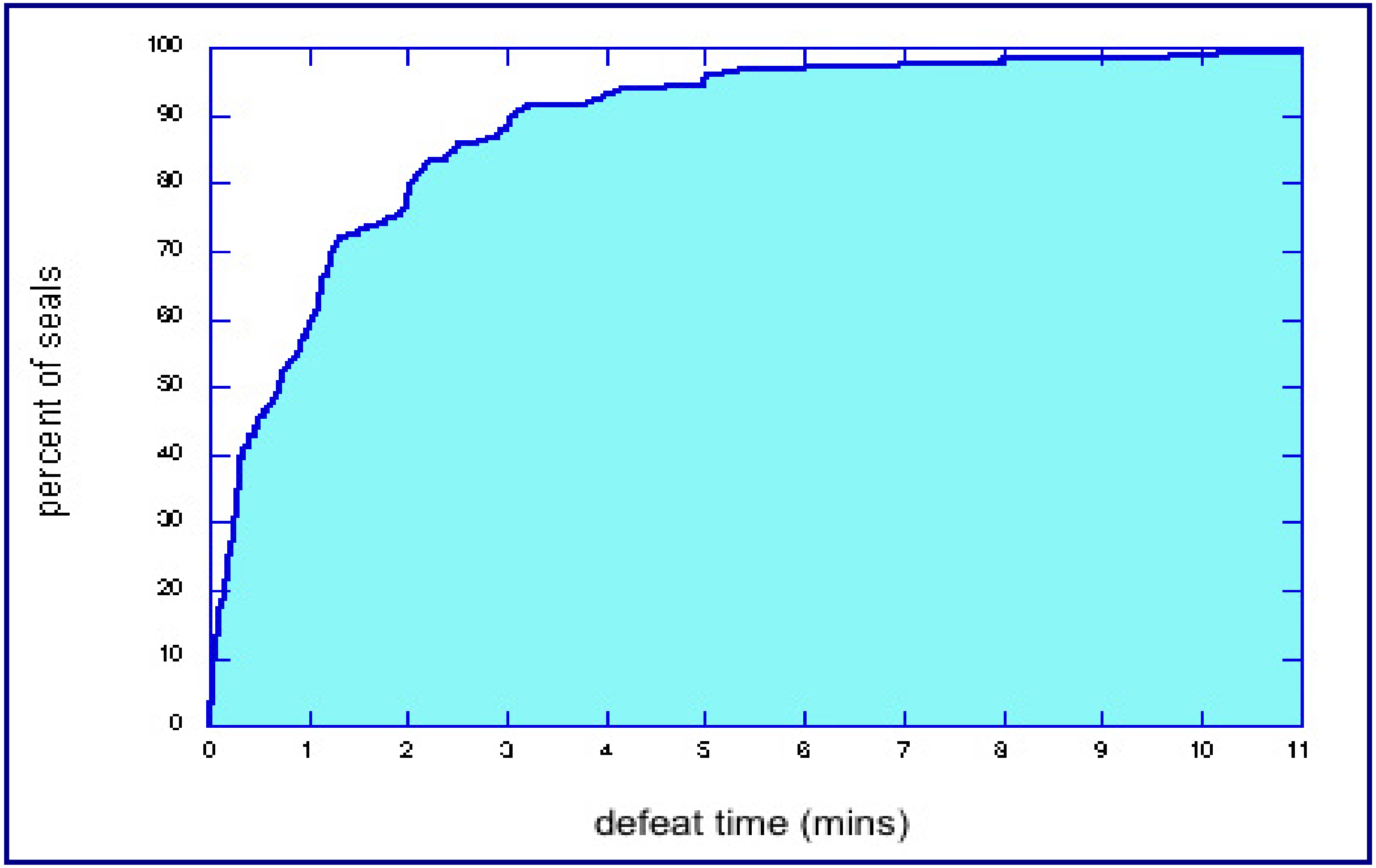
Seals Vulnerability Assessment

We studied 244 different seals in detail:

- government & commercial
- mechanical & electronic
- low-tech through high-tech
- cost varies by a factor of 10,000

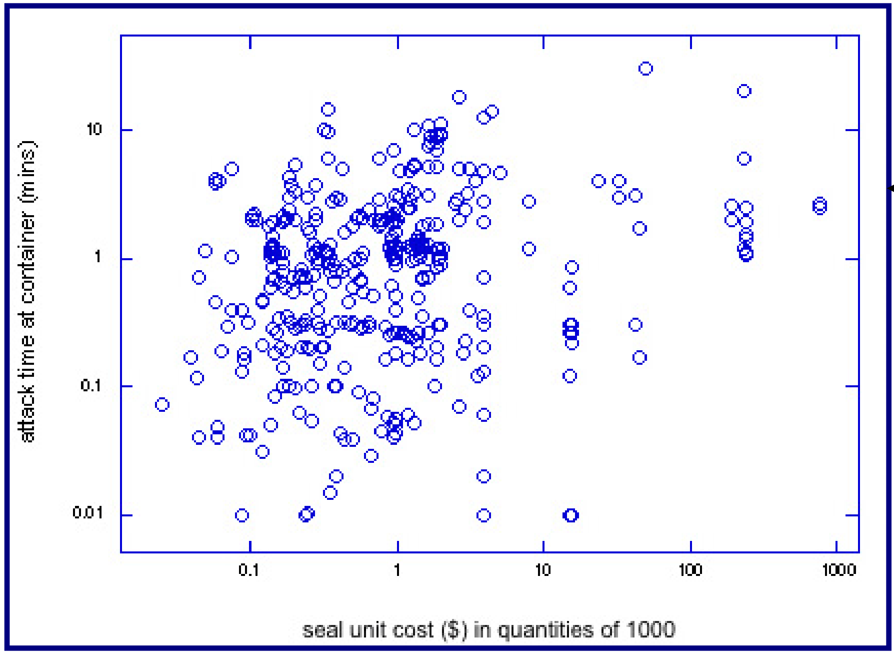
Over half are in use for critical applications, and ~19% play a role in nuclear safeguards.

Percent of Different Seal Designs That Can Be Defeated in Less Than a Given Amount of Time



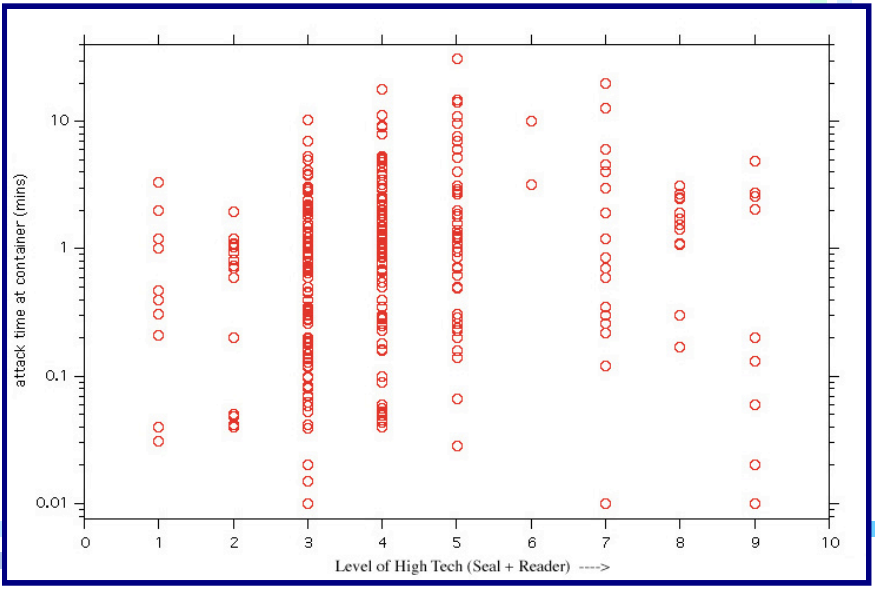
High Tech Isn't Automatically Better!

393 attacks



Linear LS fit
r = 0.10
Slope = 270 msec/$

Linear LS fit
r = 0.19
Slope = 170 msec/tech level



Results for 244 Different Seal Designs

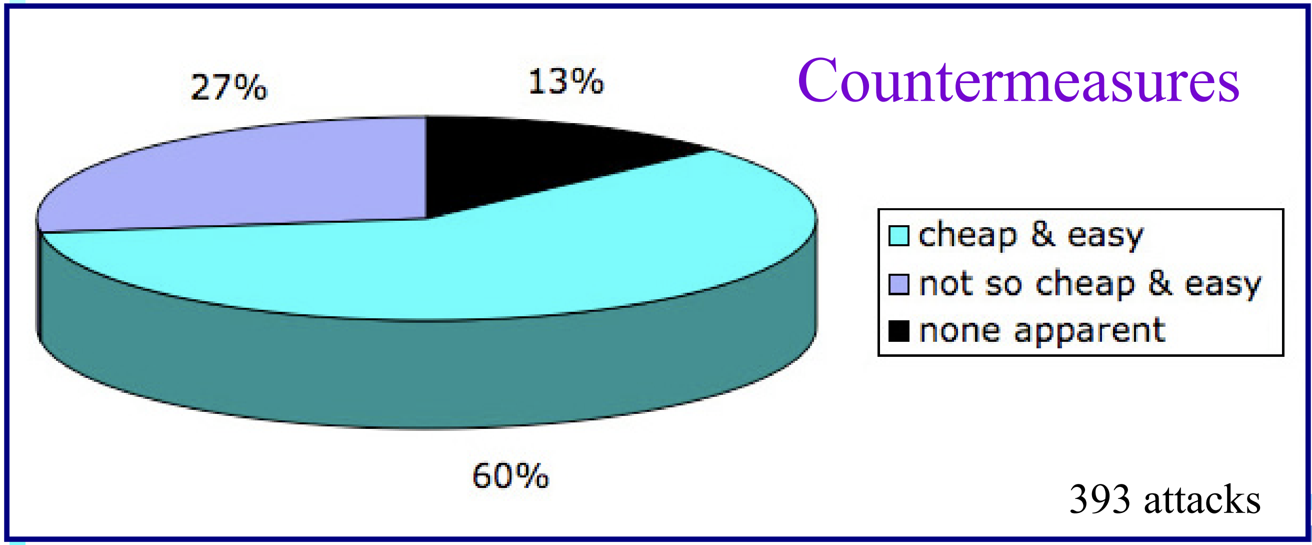
parameter	mean	median
attack time	1.4 mins	43 secs
cost of tools & supplies	$78	$5
marginal cost of attack	62¢	9¢
time to devise successful attack	2.3 hrs	12 mins

The Good News

Simple countermeasures usually exist, but require:

- understanding the seal vulnerabilities
- looking for likely attacks
- having seen examples

> The only security is the constant practice of critical thinking.
>
> -- William Graham Sumner (1840-1910)



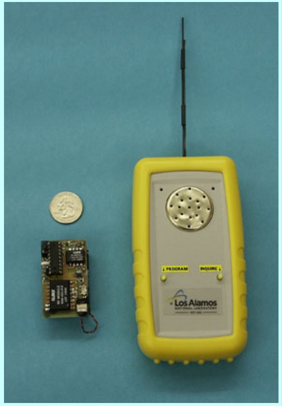
The Good News (con't)

But better seals are also possible!

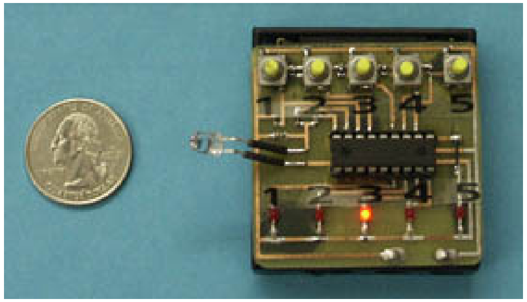
conventional seals:
They must store the fact that tampering has been detected until the seal can be inspected. But this "alarm condition" can be easily hidden or erased, or eliminated by making a fresh counterfeit seal.

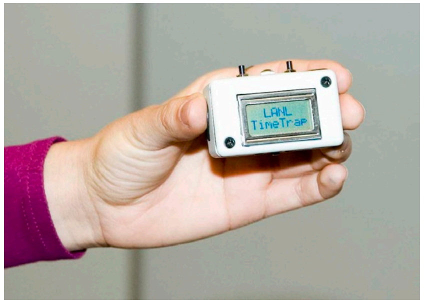
anti-evidence seals:
At the start, when the seal is first installed, store information that tampering hasn't yet been detected. Erase this "anti-evidence" when tampering is detected. This leaves nothing for an adversary to hide, erase, or counterfeit!

20+ New LANL “Anti-Evidence” Seals

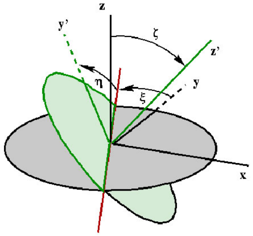


- better security
- no hasp required
- no tools to install or remove seal
- 100% reusable, even if mechanical
- the seal can go inside the container
- can monitor volumes or areas, not just portals
- can automatically verify the seal inspector actually checked the seal (“anti-gundecking”)





Effective Vulnerability Assessments



- Perform a mental coordinate transformation and pretend to be the bad guys. (This is much harder than you might think.)

- Gleefully look for trouble, rather than seeking to reassure yourself that everything is fine.

- Be much more creative than your adversaries. They need only stumble upon 1 vulnerability, you have to worry about all of them.

> It is sometimes expedient to forget who we are.
> -- Publilius Syrus (~42 BC)

VA Steps

1. Fully understand the device and how it is REALLY used. Talk to the low-level users.

2. Play with it.

3. **Brainstorm--anything goes!**

4. Play with it some more.

Nothing is like is seems, but everything is exactly like it is.
  -- Yogi Berra (baseball player & coach)

VA Steps

5. Edit & prioritize potential attacks.
6. Partially develop some attacks.
7. Determine feasibility of the attacks.
8. Devise countermeasures--more brainstorming!

You have to be careful if you don't know where you are going because you might not get there. -- Yogi Berra

VA Steps

9. Perfect attacks.
10. Demonstrate attacks.
11. Rigorously test attacks.
12. Rigorously test countermeasures.

> In theory there is no difference between theory and practice. In practice there is.
> -- Yogi Berra

Brainstorming

Nothing can inhibit and stifle the creative process more--and on this there is unanimous agreement among all creative individuals and investigators of creativity--than critical judgment applied to the emerging idea at the beginning stages of the creative process. ... More ideas have been prematurely rejected by a stringent evaluative attitude than would be warranted by any inherent weakness or absurdity in them. The longer one can linger with the idea with judgment held in abeyance, the better the chances all its details and ramifications [can emerge].

-- Eugene Raudsepp, *Managing Creative Scientists and Engineers* (1963).

Keep the possibility phase completely separate from the practicality phase!

We all know your idea is crazy. The question is, is it crazy enough? -- Niels Bohr (1885-1962)

Realities of Creativity

Individuals are creative, not groups…

but the right group dynamics can energize & encourage individuals…

and a group is usually necessary to fully explore attacks & countermeasures.

> A new idea is delicate. It can be killed by a sneer or a yawn; it can be stabbed to death by a joke or worried to death by a frown on the right person’s brow.
>
> -- Charles Brower

VA Brainstorming Tips

Pay close attention to explicit or unstated assumptions, and to security or design features that are widely praised or admired. These are often the source of serious vulnerabilities.

Concentrate on the 2nd and 3rd best attacks or countermeasures. You are likely overlooking something that would make them the best solutions.

If there is widespread agreement about an attack or countermeasure, re-examine.

No authority figures!

If everybody is thinking alike, then nobody is thinking.
-- George S. Patton (1885-1945)

VA Brainstorming Tips

> The best way to have a good idea is to have lots of ideas.
> -- Linus Pauling (1901-1994)

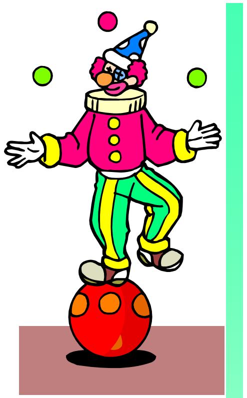
Quantity breeds quality.

With all ideas: elaborate, expand, modify, subvert, exaggerate, & combine with other ideas. Pursue hunches & intuition.

The best ideas come late, and when you are not thinking about the problem.

> Out of nowhere the idea will appear. It will come to you when you least expect it.
> -- James Webb Young

VA Brainstorming Tips



Pursue what is interesting, controversial, contrarian, exciting, or silly.

Mentally remove some design features, or pretend the seal was made of different materials. Then consider the implications.

Develop and explore models, metaphors, & analogies.

Terminology constrains our thinking. Rename everything and re-examine.

There's a fine line between fishing and just standing on the shore like an idiot.
-- Steven Wright

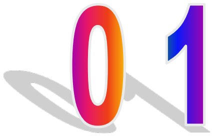
Attributes of Effective VAs

1. No conflicts of interest or wishful thinking.

2. No “Shoot the Messenger” Syndrome. No retaliation or punishment against assessors, security personnel, or managers when vulnerabilities are inevitably found.

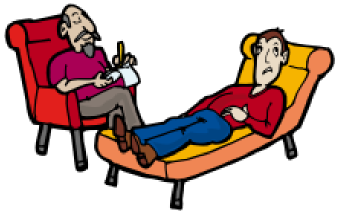
3. Rejection of a finding of zero vulnerabilities, or of VAs as some kind of “certification” or test to be passed.

4. No binary views of security.



> I don’t want any yes-men around me. I want everyone to tell me the truth, even if it costs him his job.   -- Samuel Goldwyn (1879-1974)

Attributes of Effective VAs



5. Use of independent, imaginative personnel who are psychologically predisposed to finding problems and suggesting solutions, and who (ideally) have a history of doing so.

6. Effective VA personnel tend to be: unconventional, curious, skilled with their hands, resourceful, skeptical, questioners of authority, rule benders, showoffs, praise seekers, wise guys/trouble makers.

7. The discovery of vulnerabilities is viewed as good (not bad) news.

To stimulate creativity, one must develop the childlike inclination for play and the childlike desire for recognition. -- Albert Einstein (1879-1955)

Attributes of Effective VAs

8. Done early, iteratively, and periodically.

9. Done holistically, not by component, sub-system, function, or layer. (Attacks often occur at interfaces.)

10. No unrealistic time or budget constraints, or on what attacks or adversaries can be considered.

11. Done in context.

Honest criticism is hard to take, particularly from a relative, a friend, an acquaintance, or a stranger.
-- Franklin B. Jones

Attributes of Effective VAs

12. No underestimation of the cleverness, knowledge, skills, dedication, or resources of adversaries.

13. The good guys don’t get to define the problem, the bad guys do.

14. Simple, low-tech attacks are examined first.

I don’t know a greater advantage than to appreciate the worth of an enemy.
-- Johann Wolfgang von Goethe (1749-1832)

Attributes of Effective VAs

15. Rohrbach's Maxim must be considered: No security system will ever be used properly (the way it was designed) all the time.

> Inanimate objects can be classified scientifically into three major categories; those that don't work, those that break down, and those that get lost.
>
> -- Russell Baker

16. Shannon's (Kerckhoffs') Maxim must be considered: The adversaries know and understand the security systems, strategies, and hardware being used.

> Everything secret degenerates … nothing is safe that does not show how it can bear discussion and publicity.
>
> -- Lord Acton (1834-1902)

Attributes of Effective VAs

17. Thinking about vulnerabilities & countermeasures does not end when the VA is officially over!

> A conclusion is the place where you get tired of thinking. -- Steven Wright

18. Don't overlook or under-estimate the insider threat, especially from disgruntled employees.

> If trees could scream, would we be so cavalier about cutting them down? We might, if they screamed all the time, for no good reason. -- Jack Handey

The VA Report

1. The VA Report should contain more countermeasures than are likely to be implemented.

2. The good features need to be praised.

3. Findings should be reported to the highest appropriate level without editing, interpretation, or censorship by middle managers.

The problem is not that there are problems. The problem is expecting otherwise and thinking that having problems is a problem. -- Theodore Rubin

The VA Report

4. The report should include:

- identity & experience of the assessors
- any conflict of interest
- any *a priori* constraints
- time & resources used
- samples of attacked seals
- details, videos, or demonstrations of the attacks
- time, expertise, & resources required by an adversary to execute the attacks
- possible countermeasures
- a non-sensitive, statistical summary of the findings if the sponsor wishes to take public credit for the VA

> I don’t care what is written about me as long as it isn’t true.
> -- actress Katherine Hepburn (1907-2003)